CLAIMS:

1. An apparatus for computing the sum of a divisor D_1=g.c.d. $((a_1(x)),(y-b_1(x)))$ and a divisor D_2=g.c.d. $((a_2(x)),(y-b_2(x)))$ on Jacobian of a hyperelliptic curve $y^2+y=f(x)$ defined over $GF(2^n)$, said apparatus comprising:

a storage for storing $a_1(x)$, $a_2(x)$, $b_1(x)$ and $b_2(x)$; and

means for calculating $q(x)=\{s_1(x)(b_1(x)+b_2(x))\}$ mod $a_2(x)$ or $q(x)=\{s_2(x)(b_1(x)+b_2(x))\}$ mod $a_1(x)$ by using $s_1(x)$ or $s_2(x)$ in $s_1(x)a_1(x)+s_2(x)a_2(x)=1$ in case of $GCD(a_1(x),a_2(x))=1$ where GCD denotes a greatest common divisor of two polynomials.

2. An apparatus for calculating $a'(x)$ and $b'(x)$ of a reduced divisor D'=g.c.d. $((a'(x)),(y-b'(x)))$ which is a linearly equivalent to D_1+D_2 for a divisor D_1=g.c.d. $((a_1(x)),(y-b_1(x)))$ and a divisor D_2=g.c.d. $((a_2(x)),(y-b_2(x)))$ on Jacobian of a hyperelliptic curve $y^2+y=f(x)$ defined over $GF(2^n)$, said apparatus comprising:

means for calculating $q(x)=s_1(x)(b_1(x)+b_2(x))$ mod $a_2(x)$ by using $s_1(x)$ in $s_1(x)a_1(x)+s_2(x)a_2(x)=1$ in case of

GCD($a_1(x)$,$a_2(x)$)=1 where GCD denotes a greatest common divisor of two polynomials;

means for calculating

$\alpha(x)=Q(q^2(x)a_1(x),a_2(x))+Q(f(x),a_1(x)a_2(x))$ which is rendered a monic polynomial where Q(A,B) is a quotient of A/B;

means for calculating $\beta(x)=(q(x)a_1(x)+b_1(x)+1) \bmod \alpha(x)$;

means for calculating $a'(x)=Q(f(x)+\beta^2(x),\alpha(x))$; and

means for calculating $b'(x)=(\beta(x)+1) \bmod a'(x)$.

3. An apparatus for computing the sum of a divisor D_1=g.c.d. $((a_1(x)),(y-b_1(x)))$ on Jacobian of a hyperelliptic curve $y^2+y=f(x)$ defined over $GF(2^n)$, said apparatus comprising:

a storage for storing $a_1(x)$, and $b_1(x)$; and

means for calculating $q(x)=Q(b_1^2(x)+f(x) \bmod a_1^2(x),a_1(x))$ where Q(A,B) is a quotient of A/B.

4. An apparatus for calculating a'(x) and b'(x) of a reduced divisor D'=g.c.d. ((a'(x)),(y-b'(x))) which is a linearly equivalent to D_1+D_1 for a divisor D1=g.c.d. $((a_1(x)),(y-b_1(x)))$ on Jacobian of a hyperelliptic curve

$y^2+y=f(x)$ defined over $GF(2^n)$, said apparatus comprising:

means for calculating $q(x)=Q(b_1^2(x)+f(x) \bmod a_1^2(x), a_1(x))$ where $Q(A,B)$ is a quotient of A/B;

means for calculating $\alpha(x)=q^2(x)+Q(f(x), a_1^2(x))$ which is rendered a monic polynomial;

means for calculating $\beta(x)=(b_1^2(x)+f(x) \bmod a_1^2(x)+1) \bmod \alpha(x)$;

means for calculating $a'(x)=Q(f(x)+\beta^2(x), \alpha(x))$; and

means for calculating $b'(x)=(\beta(x)+1) \bmod a'(x)$.

5. A method for calculating $a'(x)$ and $b'(x)$ of a reduced divisor $D'=g.c.d.((a'(x)),(y-b'(x)))$ which is a linearly equivalent to D_1+D_2 for a divisor $D_1=g.c.d.((a_1(x)),(y-b_1(x)))$ and a divisor $D_2=g.c.d.((a_2(x)),(y-b_2(x)))$ on Jacobian of a hyperelliptic curve $y^2+y=f(x)$ defined over $GF(2^n)$, said method comprising the steps of:

calculating and storing in a storage $q(x)=\{s_1(x)(b_1(x)+b_2(x))\} \bmod a_2(x)$ by using $s_1(x)$ in $s_1(x)a_1(x)+s_2(x)a_2(x)=1$ in case of $GCD(a_1(x), a_2(x))=1$ where GCD denotes a greatest common divisor of two polynomials;

calculating and storing in a storage $\alpha(x)=Q(q^2(x)a_1(x),a_2(x))+Q(f(x),a_1(x)a_2(x))$ which is rendered a monic polynomial where Q(A,B) is a quotient of A/B;

calculating and storing in a storage □□ $\beta(x)=(q(x)a_1(x)+b_1(x)+1) \bmod \alpha(x)$;

calculating and storing in a storage $a'(x)=Q(f(x)+\beta^2(x),\alpha(x))$; and

calculating and storing in a storage $b'(x)=(\beta(x)+1) \bmod a'(x)$.

6. A method for calculating a'(x) and b'(x) of a reduced divisor D'=g.c.d. ((a'(x)),(y-b'(x))) which is a linearly equivalent to D_1+D_1 for a divisor D1=g.c.d. $((a_1(x)),(y-b_1(x)))$ on Jacobian of a hyperelliptic curve $y^2+y=f(x)$ defined over $GF(2^n)$, said method comprising the steps of:

calculating and storing in a storage $q(x)=Q(b_1^2(x)+f(x) \bmod a_1^2(x),a_1)$ where Q(A,B) is a quotient of A/B;

calculating and storing in a storage $\alpha(x)=q^2(x)+Q(f(x), a_1^2(x))$ which is rendered a monic polynomial;

calculating and storing in a storage $\beta(x)=(b_1^2(x)+f(x) \bmod a_1^2(x)+1) \bmod \alpha(x)$;

calculating and storing in a storage $a'(x)=Q(f(x)+\beta^2(x), \alpha(x))$; and

calculating and storing in a storage $b'(x)=(\beta(x)+1) \bmod a'(x)$.

7. A method for computing the sum of a divisor D1=g.c.d. $((a_1(x)),(y-b_1(x)))$ and a divisor D_2=g.c.d. $((a_2(x)),(y-b_2(x)))$ on Jacobian of a hyperelliptic curve $y^2+y=f(x)$ defined over $GF(2^n)$, said method comprising the steps of:

storing $a_1(x)$, $a_2(x)$, $b_1(x)$ and $b_2(x)$; and

calculating and storing in a storage $q(x)=s_1(x)(b_1(x)+b_2(x)) \bmod a_2(x)$ or $q(x)=\{s_2(x)(b_1(x)+b_2(x))\} \bmod a_1(x)$ by using $s_1(x)$ or $s_2(x)$ in $s_1(x)a_1(x)+s_2(x)a_2(x)=1$ in case of $GCD(a_1(x),a_2(x))=1$.

8. A method for computing the sum of a divisor D_1=g.c.d. $((a_1(x)),(y-b_1(x)))$ on Jacobian of a hyperelliptic curve $y^2+y=f(x)$ defined over $GF(2^n)$, said method comprising the

steps of:

storing $a_1(x)$, and $b_1(x)$; and

calculating and storing in a storage $q(x)=Q(b_1^2(x)+f(x)$ mod $a_1^2(x), a_1(x))$ where $Q(A,B)$ is a quotient of A/B.